BUNDESREPUBLIK DEUTSCHLAND

19. 11. 03

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 56 587.2

Anmeldetag: 4. Dezember 2002

Anmelder/Inhaber: Philips Intellectual Property & Standards GmbH, Hamburg/DE

(vormals: Philips Corporate Intellectual Property GmbH)

Bezeichnung: Datenverarbeitungseinrichtung, insbesondere elektronisches Speicherbauteil, und hierauf bezogenes Verschlüsselungsverfahren

IPC: G 06 F 12/14

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 6. Oktober 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

A 9161
02/00
EDV-L

ZUSAMMENFASSUNG

Datenverarbeitungseinrichtung, insbesondere elektronisches Speicherbauteil, und hierauf bezogenes Verschlüsselungsverfahren

Um eine Datenverarbeitungseinrichtung, insbesondere elektronisches Speicherbauteil, aufweisend mehrere zugangsgesicherte Teilbereiche, insbesondere mehrere zugangsgesicherte Speicherbereiche, mit jeweils mindestens einem zugeordneten Parameter (a_n, a_{n-1}, ..., a_1, a_0), insbesondere Adressierung, sowie ein Verfahren zum Verschlüsseln mindestens eines Parameters (a_n, a_{n-1}, ..., a_1, a_0), insbesondere der Adressierung, mindestens eines zugangsgesicherten Teilbereichs, insbesondere mindestens eines zugangsgesicherten Speicherbereichs, mindestens einer Datenverarbeitungseinrichtung, insbesondere mindestens eines elektronischen Speicherbauteils, so weiterzubilden, dass einerseits die Sicherheit derartiger Einrichtungen in maßgeblicher Weise erhöht wird und andererseits der hiermit verbundene Aufwand sowie die technische Komplexität nicht zu hoch sind, wird vorgeschlagen, dass der Parameter (a_n, a_{n-1}, ..., a_1, a_0) mindestens eines Teilbereichs nur bereichsweise, das heißt in Abhängigkeit mindestens eines weiteren Teilbereichs verschlüsselbar (a'_n, a'_{n-1}, ..., a'_1, a'_0) ist.

Fig. 1

PHDE020290

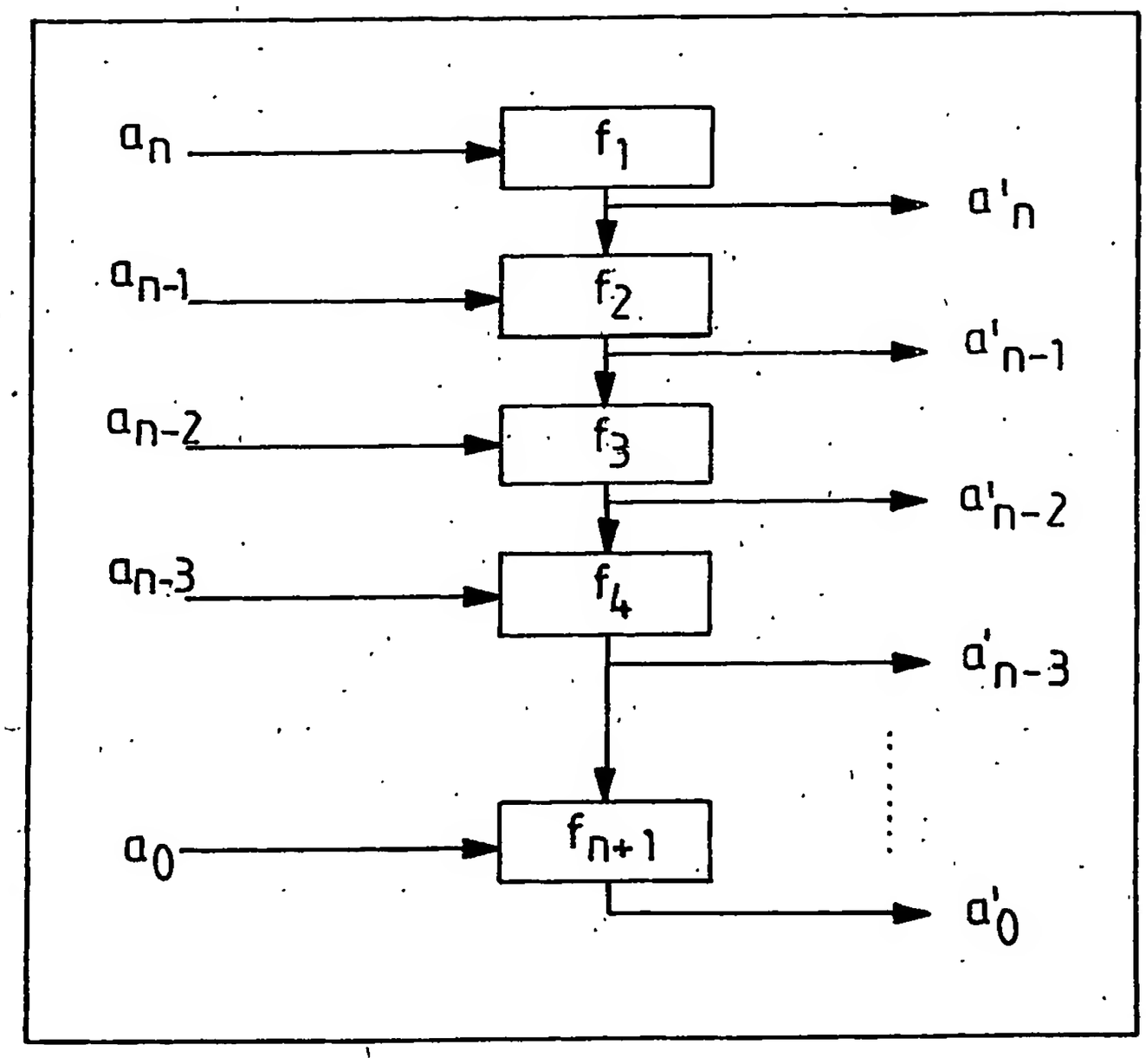

Fig.1

BESCHREIBUNG

Datenverarbeitungseinrichtung, insbesondere elektronisches Speicherbauteil, und hierauf bezogenes Verschlüsselungsverfahren

Die vorliegende Erfindung betrifft eine Datenverarbeitungseinrichtung, insbesondere ein elektronisches Speicherbauteil, aufweisend mehrere zugangsgesicherte Teilbereiche, insbesondere mehrere zugangsgesicherte Speicherbereiche, mit jeweils mindestens einem zugeordneten Parameter (a_n, a_{n-1}, ..., a_1, a_0), insbesondere Adressierung.

Die vorliegende Erfindung betrifft des weiteren ein Verfahren zum Verschlüsseln mindestens eines Parameters (a_n, a_{n-1}, ..., a_1, a_0), insbesondere der Adressierung, mindestens eines zugangsgesicherten Teilbereichs, insbesondere mindestens eines zugangsgesicherten Speicherbereichs, mindestens einer Datenverarbeitungseinrichtung, insbesondere mindestens eines elektronischen Speicherbauteils.

Bei bekannten Methoden zum Verschlüsseln von geheimen Daten, wie etwa von persönlichen Daten, von Schlüsseldaten oder von anderweitig sensitiven Daten, kann eine nichtflüchtige Speichereinheit nur als kompakter physikalischer Gesamtspeicher auf mehr oder weniger feste Weise verschlüsselt werden; dies bedeutet mit anderen Worten, daß Speicher konventionellerweise nur als Gesamtheit zugangsversperrt werden können.

Diese aus dem Stand der Technik bekannte Verschlüsselungsmethodik ganzer I[ntegrated] C[ircuit]-Bereiche ist angesichts des hiermit verbundenen hohen Aufwands sowie aufgrund der technischen Komplexität und der fehlenden Flexibilität als nachteilig anzusehen. Aus diesem Grunde gibt es immer wieder Bestrebungen, alternative Methoden zum Verschlüsseln zugangsgesicherter Speicherbereiche oder anderer Teilbereiche zu entwickeln.

Werden etwa für das Ansteuern eines Speichers der Größe $M = 2^i = 2^{n+1}$ mit $i = n+1$ Adreßleitungen eben diese Adreßleitungen über den gesamten Adreßraum verschlüsselt,

so würde die Änderung einer Adreßleitung bewirken, daß sich unter Umständen mehrere Adreßleitungen ändern, und zwar auch solche Adreßleitungen, die dafür sorgen, daß eine physikalisch weit entfernte Speicherzelle adressiert wird.

Dies ist für eine Reihe von Speichertypen nicht sinnvoll; hierzu zählen insbesondere Speicher, die in Bereichen organisiert sind, wie etwa E[rasable] P[rogrammable] R[ead] O[nly]M[emory], E[lectrical]E[rasable]P[rogrammable] R[ead]O[nly]M[emory] oder Flash-Speicher. Ein Separieren der Adreßleitungen in eine Anzahl von Bereichen und ein nachfolgendes, jeweils unabhängiges Verschlüsseln der einzelnen Bereiche ist jedoch unter dem Gesichtspunkt der Sicherheit nicht ausreichend.

Ausgehend von den vorstehend dargelegten Nachteilen und Unzulänglichkeiten sowie unter Würdigung des umrissenen Standes der Technik liegt der vorliegenden Erfindung die Aufgabe zugrunde, eine Datenverarbeitungseinrichtung, insbesondere ein elektronisches Speicherbauteil, der eingangs genannten Art sowie ein hierauf bezogenes Verschlüsselungsverfahren so weiterzubilden, dass einerseits die Sicherheit derartiger Einrichtungen in maßgeblicher Weise erhöht wird und andererseits der hiermit verbundene Aufwand sowie die technische Komplexität nicht zu hoch sind.

Diese Aufgabe wird durch eine Datenverarbeitungseinrichtung, insbesondere durch ein elektronisches Speicherbauteil von nicht-flüchtigem Charakter, mit den im Anspruch 1 angegebenen Merkmalen sowie durch ein hierauf bezogenes Verfahren zum Verschlüsseln mit den im Anspruch 6 angegebenen Merkmalen gelöst. Vorteilhafte Ausgestaltungen und zweckmäßige Weiterbildungen der vorliegenden Erfindung sind in den jeweiligen Unteransprüchen gekennzeichnet.

Gemäß der Lehre der vorliegenden Erfindung wird mithin ein völlig neuartiger Ansatz zu einem bereichsweisen Verschlüsseln von Speicherinhalten geliefert, das heißt es wird eine neue Methode zum Verschlüsseln zugangsgesicherter Speichersektoren von nicht-flüchtigem Charakter und/oder anderer Teilsektoren offenbart.

Hierzu wird durch die vorliegende Erfindung ermöglicht, Teile der (Adreß-)Parameter der Speicherbereiche auf hinsichtlich des Objekts und/oder hinsichtlich des Kunden und/oder hinsichtlich des "Die" unterschiedliche Arten zu verschlüsseln. Dies bedeutet mit anderen Worten; daß einige Teilbereiche oder Sektoren der Adresse - im Unterschied zum Stand der Technik - nicht die Gesamtheit der Adressen betreffen.

Erfindungsgemäß wird also die Verschlüsselung eines zugangsgesicherten Teilbereichs, insbesondere eines zugangsgesicherten Speicherbereichs, unter Berücksichtigung der jeweils zur Verfügung stehenden anderen Teilbereiche, insbesondere Speicherbereiche, vorgenommen. Hierdurch wird es ermöglicht, jeden Unterbereich mit jeweils anderen Parametern zu verschlüsseln.

Gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung kann eine unverschlüsselte Adresse der Form a_n, a_{n-1}, ..., a_1, a_0 gemäß vorbeschriebener Methodik zum Verschlüsseln wie folgt aussehen:

$f_1(a_n)$, $f_2(f_1(a_n)+a_{n-1})$, $f_3(f_2(f_1(a_n)+a_{n-1})+a_{n-2})$, ..., $f_{n+1}(f_n(f_{n-1}(...)))$,

das heißt eine unverschlüsselte Adresse der Form a_n, a_{n-1}, ..., a_1, a_0 kann auf $i = n+1$ (scramble-)Funktionen f_i abgebildet werden.

In diesem Zusammenhang ist ersichtlich, daß ein Variieren des Parameters a_n, insbesondere des Adressierungsparameters, zwar Einfluß auf alle anderen Adreßleitungen haben kann, ein Variieren des Parameters a_{n-1} jedoch keinen Einfluß auf die höchstwertige Funktion $f_1(a_n)$ hat.

Zweckmäßigerweise kann $f_i(a)$ eine beliebige eineindeutige Funktion sein, das heißt es gibt genau 2^i Plain-Cipher-Paare, wobei eine unverschlüsselte Adresse a_n, a_{n-1}, ..., a_1, a_0 stets in eine einmalige verschlüsselte Adresse a'_n, a'_{n-1}, ..., a'_1, a'_0 transformiert wird. Die Funktion f_i selbst muß dagegen nicht bijektiv sein, das heißt sie muß nicht umkehrbar gewählt sein.

In einer vorteilhaften Weiterbildung der vorliegenden Erfindung müssen nicht alle Stufen voll ausgeführt sein, das heißt einige Funktionen f_i können das betreffende Adreßbit direkt wiedergeben: $a' = a$. Alternativ oder in Ergänzung hierzu können die Adreßbits auch gruppiert werden; dies kann in zweckmäßiger Weise unter anderem bedeuten, daß die Inputs an die Funktionen f_i sowie die Rückgabewerte von den Funktionen f_i mehrere Bit breit sein können.

In einer vorteilhaften Ausgestaltung der vorliegenden Erfindung ist

- für EPROM-Speicher oder für EEPROM-Speicher eine Aufteilung in zwei Teilbereiche mit Funktionen $f_1(a_n, ..., a_x)$ und $f_2(f_1(a_{x-1}, ..., a_0))$ und
- für Flash-Speicher eine Aufteilung in drei Teilbereiche mit Funktionen $f_1(a_n, ..., a_x)$, $f_2(f_1(a_{x-1}, ..., a_y))$ und $f_3(f_2(f_1(a_{y-1}, ..., a_0)))$

nutzbar.

Gemäß einer besonders erfinderischen Weiterbildung können zugangsgesicherte Speicherbereiche getrennt bzw. separat gesichert werden, das heißt Randbedingungen, die einen physikalischen Speicher bedingen, werden durch die neue Methode vollständig ausgenutzt (die Vielfalt der Verschlüsselungen wird hierbei nur in unwesentlicher Weise eingeschränkt).

Die vorliegende Erfindung betrifft des weiteren einen Mikrocontroller, insbesondere SmartCard-Controller, aufweisend mindestens eine Datenverarbeitungseinrichtung gemäß der vorstehend dargelegten Art. Dementsprechend kann die vorbeschriebene Methode in bevorzugter Weise zum Beispiel in alle SmartCard-Entwicklungen eingebaut werden.

Die vorliegende Erfindung betrifft schließlich die Verwendung mindestens einer Datenverarbeitungseinrichtung, insbesondere mindestens eines elektronischen Speicherbauteils, gemäß der vorstehend dargelegten Art in mindestens einer Chipeinheit, insbesondere in mindestens einem SmartCard-Controller, in mindestens einem Reader-I[ntegrated] C[ircuit] oder in mindestens einem Kryptochipsatz, zum Beispiel im Bereich der Audio- und/oder Video-Verschlüsselung.

Wie bereits vorstehend erörtert, gibt es verschiedene Möglichkeiten, die Lehre der vorliegenden Erfindung in vorteilhafter Weise auszugestalten und weiterzubilden. Hierzu wird einerseits auf die dem Anspruch 1 sowie dem Anspruch 6 nachgeordneten Ansprüche verwiesen, andererseits werden weitere Ausgestaltungen, Merkmale und Vorteile der vorliegenden Erfindung nachstehend anhand des durch Figur 1 veranschaulichten Ausführungsbeispiels näher erläutert.

Es zeigt:

Fig. 1 in schematischer Blockdarstellung ein Ausführungsbeispiel für das auf eine Datenverarbeitungseinrichtung gemäß der vorliegenden Erfindung angewandte Verschlüsselungsverfahren gemäß der vorliegenden Erfindung.

Das zur Anwendung in einem elektronischen Speicherbauteil gelangende Verschlüsselungsverfahren gemäß der vorliegenden Erfindung beruht darauf, daß unverschlüsselte Adressen a_n, a_{n-1}, ..., a_1, a_0 eines zugangsgesicherten Speicherbereichs nur bereichsweise, das heißt in Abhängigkeit von einem oder mehreren weiteren Speicherbereichen verschlüsselt werden, so daß verschlüsselte Adressen a'_n, a'_{n-1}, ..., a'_1, a'_0 gebildet werden.

Hierzu sind $i = n+1$ eineindeutige ($\dashrightarrow 2^i = 2^{n+1}$ Plain-Cipher-Paare) scramble-Funktionen f_1, f_2, ..., f_n, f_{n+1} vorgesehen, so daß die unverschlüsselten Adressen der Form a_n, a_{n-1}, ..., a_1, a_0 nach Abbilden durch die Funktionen f_i verschlüsselt folgendermaßen aussehen (vgl. Figur 1):

$f_1(a_n)$, $f_2(f_1(a_n)+a_{n-1})$, $f_3(f_2(f_1(a_n)+a_{n-1})+a_{n-2})$, ..., $f_{n+1}(f_n(f_{n-1}(...)))$

Hierdurch wird es ermöglicht, jeden Unterbereich mit jeweils anderen Parametern zu verschlüsseln.

In diesem Zusammenhang ist ersichtlich, daß eine Variation der Adressen a_n, a_{n-1}, ..., a_1, a_0 zwar Einfluß auf alle anderen Adreßleitungen haben kann, eine Variation des Parameters a_{n-1} jedoch keinen Einfluß auf die höchstwertige Funktion $f_1(a_n)$.

Alternativ zur Darstellung gemäß Figur 1 müssen nicht alle $i = n+1$ Stufen voll ausgeführt sein, das heißt einige Funktionen f_i können das betreffende Adreßbit auch direkt wiedergeben: $a' = a$.

Des weiteren können die Adreßbits auch gruppiert werden; dies kann unter anderem bedeuten, daß die Inputs an die Funktionen f_i sowie die Rückgabewerte von den Funktionen f_i mehrere Bit breit sein können.

BEZUGSZEICHENLISTE

a_0	erste unverschlüsselte Adresse
a_1	zweite unverschlüsselte Adresse
a_{n-1}	n.te unverschlüsselte Adresse
a_n	n+1.te unverschlüsselte Adresse
a'_0	erste verschlüsselte Adresse
a'_1	zweite verschlüsselte Adresse
a'_{n-1}	n.te verschlüsselte Adresse
a'_n	n+1.te verschlüsselte Adresse
f_1	erste Funktion, insbesondere erste scramble-Funktion
f_2	zweite Funktion, insbesondere zweite scramble-Funktion
f_n	n.te Funktion, insbesondere n.te scramble-Funktion
f_{n+1}	n+1.te Funktion, insbesondere n+1.te scramble-Funktion

PATENTANSPRÜCHE

1. Datenverarbeitungseinrichtung, insbesondere elektronisches Speicherbauteil, aufweisend mehrere zugangsgesicherte Teilbereiche, insbesondere mehrere zugangsgesicherte Speicherbereiche, mit jeweils mindestens einem zugeordneten Parameter (a_n, a_{n-1}, ..., a_1, a_0), insbesondere Adressierung,

dadurch gekennzeichnet,

dass der Parameter (a_n, a_{n-1}, ..., a_1, a_0) mindestens eines Teilbereichs nur bereichsweise, das heißt in Abhängigkeit mindestens eines weiteren Teilbereichs verschlüsselbar (a'_n, a'_{n-1}, ..., a'_1, a'_0) ist.

2. Datenverarbeitungseinrichtung gemäß Anspruch 1,

dadurch gekennzeichnet,

dass der zu verschlüsselnde Parameter (a_n, a_{n-1}, ..., a_1, a_0) in Abhängigkeit, insbesondere als Funktion ($f_1(a_n)$, $f_2(f_1(a_n),a_{n-1})$, ..., $f_n(f_{n-1}(...))$, $f_{n+1}(f_n(f_{n-1}(...)))$), mindestens eines Parameters des weiteren Teilbereichs verschlüsselbar (a'_n, a'_{n-1}, ..., a'_1, a'_0) ist.

3. Datenverarbeitungseinrichtung gemäß Anspruch 2,

dadurch gekennzeichnet,

dass

- der Eingabewert (a_n, a_{n-1}, ..., a_1, a_0) an die Funktion (f_i) und/oder
- der Rückgabewert (a'_n, a'_{n-1}, ..., a'_1, a'_0) von der Funktion (f_i)

mehr als ein Bit breit ist.

4. Datenverarbeitungseinrichtung gemäß mindestens einem der Ansprüche 1 bis 3;
dadurch gekennzeichnet,
dass das Speicherbauteil
- als E[rasable] P[rogrammable]R[ead]O[nly]M[emory],
- als E[lectrical]E[rasable] P[rogrammable]R[ead]O[nly]M[emory] oder
- als Flash-Speicher

ausgebildet ist.

5. Mikrocontroller, insbesondere SmartCard-Controller, aufweisend mindestens eine Datenverarbeitungseinrichtung gemäß mindestens einem der Ansprüche 1 bis 4.

6. Verfahren zum Verschlüsseln mindestens eines Parameters (a_n, a_{n-1}, ..., a_1, a_0), insbesondere der Adressierung, mindestens eines zugangsgesicherten Teilbereichs, insbesondere mindestens eines zugangsgesicherten Speicherbereichs, mindestens einer Datenverarbeitungseinrichtung, insbesondere mindestens eines elektronischen Speicherbauteils,
dadurch gekennzeichnet,
dass der zu verschlüsselnde Parameter (a_n, a_{n-1}, ..., a_1, a_0) des Teilbereichs nur bereichsweise, das heißt in Abhängigkeit mindestens eines weiteren Teilbereichs verschlüsselt (a'_n, a'_{n-1}, ..., a'_1, a'_0) wird.

7. Verfahren gemäß Anspruch 6,
dadurch gekennzeichnet,
dass der zu verschlüsselnde Parameter (a_n, a_{n-1}, ..., a_1, a_0) des Teilbereichs in Abhängigkeit, insbesondere als Funktion ($f_1(a_n)$, $f_2(f_1(a_n), a_{n-1}$, ..., $f_n(f_{n-1}(...))$, $f_{n+1}(f_n(f_{n-1}(...)))$, mindestens eines Parameters des weiteren Teilbereichs verschlüsselt (a'_n, a'_{n-1}, ..., a'_1, a'_0) wird.

8. Verfahren gemäß Anspruch 7,

dadurch gekennzeichnet,

dass die Funktion $f_i(a)$ eineindeutig ist.

9. Verfahren gemäß mindestens einem der Ansprüche 6 bis 8,

dadurch gekennzeichnet,

dass die zugangsgesicherten Teilbereiche, insbesondere die zugangsgesicherten Speicherbereiche, getrennt bzw. separat gesichert werden.

10. Verwendung mindestens einer Datenverarbeitungseinrichtung, insbesondere mindestens eines elektronischen Speicherbauteils, gemäß mindestens einem der Ansprüche 1 bis 4 in mindestens einer Chipeinheit, insbesondere

- in mindestens einem SmartCard-Controller,
- in mindestens einem Reader-I[ntegrated]C[ircuit] oder
- in mindestens einem Kryptochipsatz,

zum Beispiel im Bereich der Audio- und/oder Video-Verschlüsselung.

PHDE020290

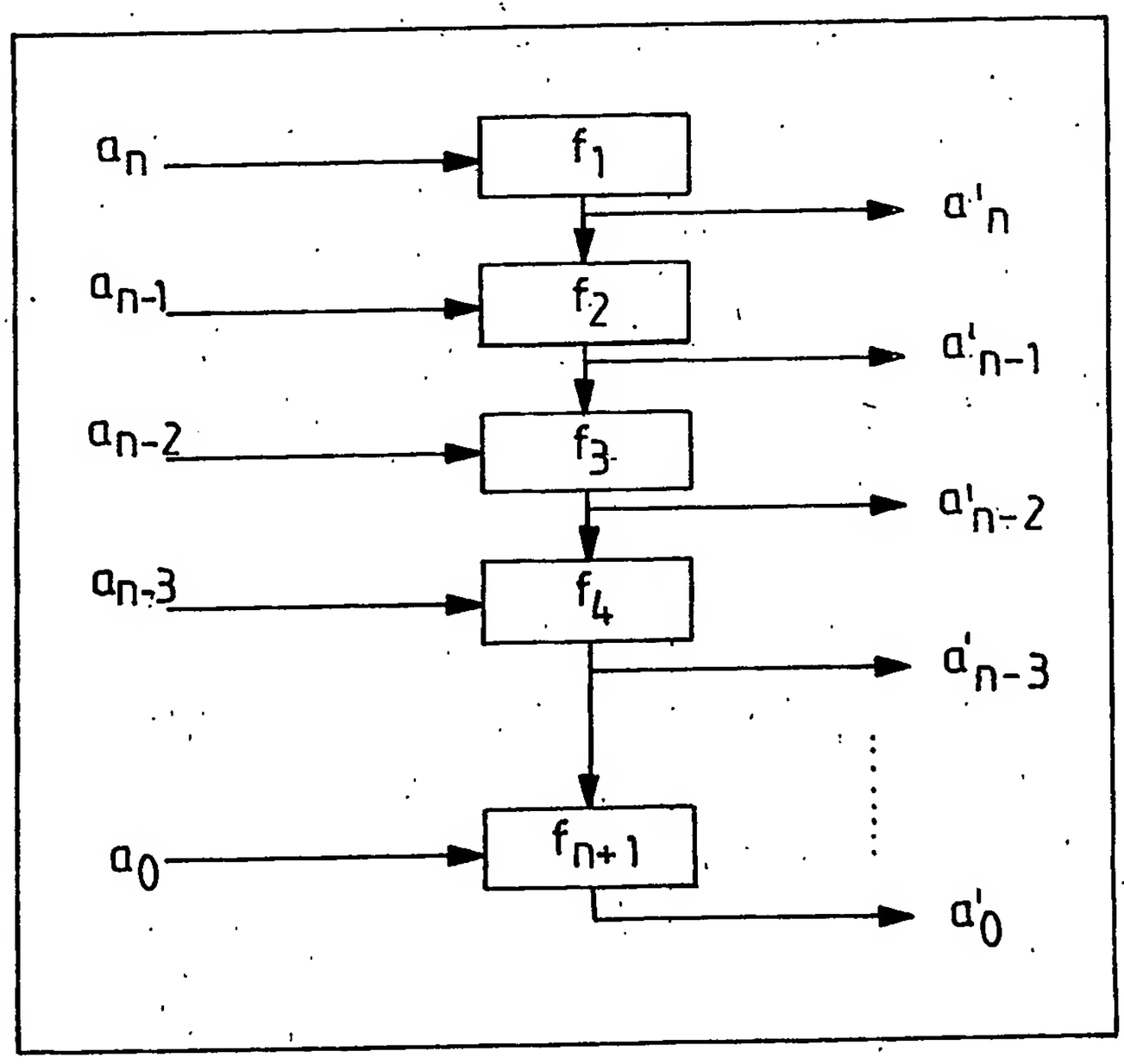

Fig.1